PROGRAMA DE CURSO
TALLER DE HACKING COMPETITIVO

A. Antecedentes generales del curso:

Departamento	Ciencias de la Computación					
Nombre del curso	Taller de Hacking Competitivo	**Código**	CC5325	**Créditos**	6	
Nombre del curso en inglés	Competitive Hacking Workshop					
Horas semanales	**Docencia**	3,0	**Auxiliares**	2,0	**Trabajo personal**	5,0
Carácter del curso	**Obligatorio**		**Electivo**	X		
Requisitos	CC3001					

B. Propósito del curso:

El curso busca motivar el interés y mejorar la comprensión de los y las estudiantes sobre conceptos de seguridad computacional (ciberseguridad) a través de actividades competitivas denominadas *Capture the Flag (CTF).*

Capture The Flag es una actividad en la cual un equipo, trabajando coordinadamente, resuelve desafíos de ciberseguridad en particular y computación en general, basados en programación, ingenio, deducción lógica, matemática básica, ingeniería reversa, entre otros, para lograr una meta (recuperar o modificar un valor en un sistema dado).

El curso tributa a las siguientes competencias específicas (CE) y genéricas (CG) del Plan de Formación de Ingeniería Civil en Computación:

CE4: Extraer información relevante, utilizando el proceso de descubrimiento de conocimiento de datos.

CE6: Desarrollar software en una amplia variedad de plataformas y lenguajes de programación.

CE8: Diagnosticar y resolver problemas en el funcionamiento de software cercano a la plataforma para mejorar su desempeño.

CG1 (Comunicación académica y profesional): Comunicar en español de forma estratégica, clara y eficaz, tanto en modalidad oral como escrita, puntos de vista, propuestas de proyectos y resultados de investigación fundamentados, en situaciones de comunicación compleja, en ambientes sociales, académicos y profesionales.

CG3 (Compromiso ético): Actuar de manera responsable y honesta, dando cuenta en forma crítica de sus propias acciones y sus consecuencias, en el marco del respeto hacia la dignidad de las personas y el cuidado del medio social, cultural y natural.

CG4 (Trabajo en equipo): Trabajar en equipo, de forma estratégica y colaborativa, en diversas actividades formativas, a partir de la autogestión de sí mismo y de la relación con el otro, interactuando con los demás en diversos roles: de líder, colaborador u otros, según requerimientos u objetivos del trabajo, sin discriminar por género u otra razón.

C. Resultados de aprendizaje:

Competencias específicas	Resultados de aprendizaje
CE4, CE6, CE8	**RA1:** Resuelve problemas característicos de competencias del tipo *Capture the Flag,* usando conocimientos básicos de esteganografía y criptografía clásica y moderna.
CE4, CE6, CE8	**RA2:** Resuelve problemas característicos de competencias del tipo *Capture the Flag,* usando conocimientos básicos de implementación y uso de aplicaciones web y de escritorio, además de su análisis forense, ingeniería reversa y abuso de vulnerabilidades para escalamiento de privilegios *(Pwning)*.
CE4, CE6, CE8	**RA3:** Resuelve problemas característicos de competencias del tipo *Capture the Flag,* usando conocimientos básicos de inteligencia de fuentes abiertas *(OSINT)*
Competencias genéricas	**Resultados de aprendizaje**
CG3	**RA4:** Actúa con responsabilidad y honestidad al momento de utilizar los conocimientos adquiridos, realizando estas acciones solamente en sistemas en los que cuenta con autorización explícita o como parte de un proceso cuidadoso de notificación coordinada de vulnerabilidades, siguiendo las buenas prácticas y recomendaciones estándares de la industria.
G1	**RA5:** Genera documentación de forma detallada, comprensible y reproducible sobre el proceso de razonamiento utilizado para resolver problemas de tipo *Capture the Flag.*
CG4	**RA6:** Trabaja en equipo para resolver de forma coordinada problemas de tipo *Capture the Flag*.

D. Unidades temáticas:

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
1	**RA1, RA5, RA6**	Introducción al CTF y Problemas de Esteganografía	2 semanas
Contenidos		**Indicador de logro**	
1 Introducción a los CTF: Habilidades básicas, codificaciones, cifrados básicos, flags, reglas comunes y código de conducta. 2 Técnicas para realizar esteganografía en archivos de imagen, sonido y texto. 3 Otros tipos de técnicas esteganográficas.		El o la estudiante: 1 Explica en términos generales el funcionamiento de los CTFs, sus reglas comunes y su código de conducta. 2 Identifica las codificaciones más usadas en CTFs. 3 Utiliza de forma adecuada las herramientas necesarias para resolver problemas básicos de esteganografía. 4 Resuelve problemas básicos de esteganografía típicos de competencias del tipo CTFs de forma grupal. 5 Elabora de forma individual documentación clara y detallada de los pasos a seguir para resolver problemas de esteganografía en CTFs.	
Bibliografía de la unidad		[9] (Capítulo 21), [2], [7]	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
2	**RA1, RA5, RA6**	Problemas de Criptografía Moderna	2 semanas
Contenidos		**Indicador de logro**	
1 Criptografía Simétrica y Asimétrica. 2 Encriptación y Firmado, tanto en los casos simétrico como asimétrico. 3 Funciones de Hash. 4 Errores comunes de implementación de funciones y esquemas criptográficos.		El o la estudiante: 1 Explica conceptos básicos de criptografía, así como también puntos críticos en su implementación que pudiesen ser aprovechados en el contexto de un problema de CTF. 2 Utiliza de forma correcta librerías criptográficas para programar herramientas que permiten resolver problemas básicos sobre criptografía usuales en CTFs. 3 Resuelve problemas básicos sobre criptografía en CTFs de forma grupal. 4 Elabora de forma individual documentación clara y detallada de los pasos a seguir para resolver problemas de criptografía moderna	

	en CTFs.
Bibliografía de la unidad	[2],[3]

Número	**RA al que tributa**	**Nombre de la unidad**	**Duración en semanas**
3	**RA2, RA5, RA6**	Problemas de Aplicaciones Web	2 semanas

Contenidos	**Indicador de logro**
1 Partes de una aplicación web. 2 Detección de bugs y versiones obsoletas. 3 Vulnerabilidades Comunes de aplicaciones web. 4 Explotación de vulnerabilidades web.	El o la estudiante: 1 Describe las distintas partes que componen una aplicación web. 2 Analiza adecuadamente el software y la versión de algunos tipos de aplicaciones web populares. 3 Utiliza de forma correcta herramientas comunes para detectar y explotar vulnerabilidades en aplicaciones web de CTFs. 4 Resuelve problemas básicos sobre aplicaciones web en CTFs de forma grupal. 5 Elabora de forma individual documentación clara y detallada de los pasos a seguir para resolver problemas de aplicaciones web en CTFs.
Bibliografía de la unidad	[2], [4], [6], [10]

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
4	**RA2, RA5, RA6**	Problemas de Análisis Forense	2 semanas

Contenidos	Indicador de logro
1 Análisis forense sobre logs. 2 Análisis forense sobre tráfico de red (capturas de paquetes). 3 Análisis forense sobre máquinas virtuales.	El o la estudiante: 1 Explica los conceptos básicos de análisis forense y las características comunes de problemas de análisis forense usuales de CTFs. 2 Utiliza correctamente las principales herramientas forense populares para realizar análisis forense básico sobre logs, tráfico de red, y máquinas virtuales. 3 Resuelve problemas básicos de análisis forense en CTFs de forma grupal. 4 Elabora de forma individual documentación clara y detallada de los pasos a seguir para resolver problemas de análisis forense en CTFs.
Bibliografía de la unidad	[9], [13]

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
5	**RA2, RA5, RA6**	Problemas de Ingeniería Reversa	2 semanas
Contenidos		**Indicador de logro**	
1 Introducción a la ingeniería reversa. 2 Técnicas para realizar ingeniería reversa. 3 Técnicas de ofuscación comunes y sus contramedidas.		El o la estudiante: 1 Explica en términos generales el funcionamiento de las herramientas de ingeniería reversa sobre aplicaciones de escritorio. 2 Utiliza adecuadamente herramientas comunes para realizar ingeniería reversa sobre aplicaciones de escritorio en CTFs. 3 Resuelve problemas básicos de ingeniería reversa en CTFs de forma individual y grupal. 4 Elabora de forma individual documentación clara y detallada de los pasos a seguir para resolver problemas de ingeniería reversa en CTFs.	
Bibliografía de la unidad		[1], [2], [5], [8]	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
6	**RA2, RA5, RA6**	Problemas de *Pwning*	3 semanas
Contenidos		**Indicador de logro**	
1 Introducción al *Pwning* y Ataques de control de flujo 2 Ejecución de ataques de escalamiento de privilegios.		El o la estudiante: 1 Explica en términos generales ataques básicos de control de flujo, que permiten resolver problemas de toma de control de aplicaciones (*Pwning*) en CTFs. 2 Resuelve problemas básicos de tipo *Pwning* en CTFs de forma grupal. 3 Elabora de forma individual documentación clara y detallada de los pasos a seguir para resolver problemas de *Pwning* en CTFs.	
Bibliografía de la unidad		[2], [4], [11]	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
7	**RA3, RA4, RA5, RA6**	Problemas de *Open Source Intelligence y* participación en CTF real	2 semanas

Contenidos	Indicador de logro
1 Definiciones acerca de técnicas de *Open Source Intelligence (OSINT)* 2 Ejemplos prácticos de del uso de técnicas de *OSINT* para la obtención de datos personales. 3 Participación grupal en competencia de tipo CTF: requerimientos, reglas y código de ética.	El o la estudiante: 1 Describe en términos generales el concepto de *Open Source Intelligence* 2 Utiliza herramientas existentes o desarrolla sus propias herramientas para la resolución de problemas de tipo *Open Source Intelligence* en CTFs. 3 Resuelve problemas básicos de tipo *Open Source Intelligence* en CTFs de forma grupal. 4 Elabora de forma individual documentación clara y detallada de los pasos a seguir para resolver problemas de *Open Source Intelligence* en CTFs. 5 Utiliza los conocimientos adquiridos para la resolución de problemas de tipo CTF de forma honesta, ética y responsable, siguiendo las recomendaciones de la industria para hacerlo en contextos reales.
Bibliografía de la unidad	[12]

E. Estrategias de enseñanza:

La estrategia de enseñanza utilizada considera la realización de sesiones de discusión de problemas y resolución de consultas en horario de clases, bloques de discusión de problemas en clases auxiliares y tareas con colecciones de ejercicios para cada unidad, así como también una competencia grupal final con problemas de todos los temas vistos en el año.

- El horario de clases se usará para resolver dudas con el o la profesora de cátedra, además de proponer problemas para su resolución durante las clases.
- Las clases auxiliares se usarán principalmente para contestar dudas sobre los contenidos del curso o los problemas propuestos de tarea, además de resolver problemas colectivamente.
- Como material adicional, se entregarán videos o apuntes con base teórica necesaria para resolver los problemas a evaluar en el curso.
- Las tareas se liberarán de forma periódica y están pensadas para su resolución en equipos. Sin embargo, la entrega requerirá la elaboración individual de archivos de código y de un documento escrito denominado *writeup*, en el cual el o la estudiante describe los pasos que siguió para resolver los problemas planteados.

El curso contempla cinco horas de trabajo autónomo semanal, las cuales se deberán dedicar a la revisión individual del material adicional y a la resolución de los problemas propuestos.

F. Estrategias de evaluación:

El curso contempla dos categorías de evaluación de proceso, todas reprobatorias por sí solas; aprobar el curso requiere que la nota promedio de cada categoría sea igual o superior a 4.0. Las categorías son:

- Tareas: Incluye tareas de resolución grupal y entrega individual, consistentes en problemas de tipo *Capture the Flag*. Las tareas serán evaluadas a través de *write-ups* o descripciones escritas de los pasos seguidos para poder resolver cada problema, además de la entrega del código utilizado.
- Una evaluación grupal final. Esta consiste en una competencia abierta tipo "Capture The Flag", en la cual grupos de estudiantes competirán en vivo para obtener la mayor cantidad de *flags* posible.

La ponderación de cada evaluación respetará siempre los reglamentos de la Escuela.

G. Recursos bibliográficos:

Bibliografía Obligatoria:

El material esencial para la resolución de problemas en el curso se entregará durante su desarrollo en una página web dedicada, la cual será informada a los y las estudiantes durante la primera semana de clases.

Bibliografía recomendada:

La bibliografía siguiente puede ser de apoyo para la resolución de algunos problemas presentados en el curso:

[1] The IDA Pro Book, Chris Eagle, 2011
[2] Black Hat Python, Justin Seitz, 2014
[3] Serious Cryptography, Jean-Philippe Aumasson, 2016
[4] Metasploit, The Penetration Tester's Guide, David Kennedy et al., 2011
[5] Practical Binary Analysis, Dennis Andriesse, 2019
[6] Attacking Network Protocols, James Forshaw, 2018
[7] Linux Basics for Hackers, OccupyTheWeb, 2018
[8] Reversing: Secrets of Reverse Engineering, Eldad Eliam, 2011
[9] Introductory Computer Forensics, Xiaodong Lin, 2018
[10] OWASP Web Security Test Guide (https://owasp.org/www-project-web-security-testing-guide/)

[11] The Shellcoder's Handbook, Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte; 2011
[12] OSINT Framework (https://osintframework.com/)
[13] Wireshark for Security Professionals, Jessey Bullock & Jeff T. Parker, 2017

H. Datos generales sobre elaboración y vigencia del programa de curso:

Vigencia desde:	2021
Elaborado por:	Eduardo Riveros
Validado por:	Alejandro Hevia
Revisado por:	AGC - CTD